UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/798,079	03/11/2004	Aaron Charles Newman	AS2	5342

7590 12/22/2008

Peter S. Canelias
Law Offices of Peter S. Canelias
Suite 2148
420 Lexington Avenue
New York, NY 10170

EXAMINER	
KIM, PAUL	
ART UNIT	**PAPER NUMBER**
2169	
MAIL DATE	**DELIVERY MODE**
12/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/798,079	**Applicant(s)** NEWMAN ET AL.	
	Examiner PAUL KIM	**Art Unit** 2169	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2008*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *98-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *98-104* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the following communication: Amendment filed on 16 September 2008.

2. Claims 98-104 are pending and present for examination.

Response to Amendment

3. Claim 98 has been amended.

4. No claims have been further cancelled.

5. No claims have been newly added.

Specification

6. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required: Claims 98-104 recite "[a] computer readable medium having code to perform a computer implemented method."

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 98-104** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The claims are non-statutory because they fail to limit the claimed invention to tangible subject matter and/or embodiments which fall within a statutory category.

The claims make no mention of a tangible medium wherein existing code may be processed to perform the recited steps in the claims. See State Street, 149 F.3d at 1373, 47 USPQ2d at 1601-02.

MPEP 2106. "The claimed invention as a whole must accomplish a practical application. That is, it must produce a 'useful, concrete and tangible result' " (emphasis added).

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. **Claim 98** is rejected under 35 U.S.C. 102(b) as being anticipated by Bapat et al (U.S. Patent No. 6,038,563, hereinafter referred to as BAPAT), filed on 25 March 1998, and issued on 14 March 2000.

11. **As per independent claim 98,** BAPAT teaches:

A computer readable medium having code to perform a computer implemented method for protecting a database hosted on a server, comprising:

installing a console on a remote computer system for monitoring activity on the database {See BAPAT, C8:L17-29, wherein this reads over "each auxiliary server 152, 154 includes the same hardware and software elements found in the MIS ... [and] each have just one interface 160/166 for receiving access requests"};

presenting the installed console through a user interface {See BAPAT, C11:L39-51, wherein this reads over "[t]he Access Control Configuration procedures 210 presents a graphical user interface 212 to users authorized to modify the access control tree"};

registering a listener agent with the console {See BAPAT, C16:L66-C17:L14, wherein this reads over "[a] set of filters 291, 294, in the log server 290 determine which event notifications are stored"};

the listener agent being installed on the server hosting the database {See BAPAT, C16:L55-66, wherein this reads over "the log server" and "[t]he log server 290 is preferably a software entity or process that runs on the same computer or computer node as the MIS"};

establishing a secure connection between the console and the listener agent {See BAPAT, Figure 3};

configuring the listener agent with a first set of rules having a set of security attributes {See BAPAT, C17:L3-14, wherein this reads over "[t]his filter 291 passes "access grant" and "access denial" event notifications generated by the MIS"};

installing a collector agent to be in communication with the listener agent for collecting a plurality of database events {See BAPAT, C17:L3-14, wherein this reads over "[t]his filter 291 passes "access grant" and "access denial" event notifications generated by the MIS"};

deconstructing the plurality of database events into a plurality of atomic messages {See BAPAT, C18:L24-27, wherein this reads over "[u]ser queries requesting information from tables to which the user does not have access rights are rejected by the SQL engine"};

analyzing the plurality of atomic messages for compliance with the first set of rules {See BAPAT, C17:L15-19, wherein this reads over "a Security Alarm log 293 that is separate from the security audit trail 192, where security alarms are generated and stored in the log only when there is a denial of object access"};

executing compliant database events {See BAPAT, C18:L19-27, wherein this reads over "only queries in full compliance with those access rights are processed"; and C28:L31-37, wherein this reads over "[a]ccess is allowed only for the objects to which the user has appropriate access rights"};

sending a signal to a console operator when a database event is not compliant with the first set of rules {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"};

allowing a console operator to create exceptions to the first set of rules when signals are sent by the listener agent {See BAPAT, C11:L39-51, wherein this reads over "users authorized to modify the access control tree"};

updating the first set of rules with the exceptions created by the console operator {See BAPAT, C11:L39-51, wherein this reads over "users authorized to modify the access control tree"};

storing the signals received by the console operator in a data file residing with the console {See BAPAT, C12:L56-57, wherein this reads over "[t]he deny/grant decision for each access request may be stored in a security audit trail"}.

12. **As per independent claim 101,** BAPAT teaches:

The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:

determining whether an executable SQL statement contains a write operation to a data dictionary {See BAPAT, C6:L4-11, wherein this reads over "[i]f a suspicious directory name is found 68, the control function is notified"};

preventing the data dictionary from being written to {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

13. **Claim 99** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Shostack et al (U.S. Patent No. 6,298,445, hereinafter referred to as SHOSTACK), filed on 30 April 1998, and issued on 2 October 2001.

14. **As per dependent claim 99,** BAPAT, in combination with SHOSTACK, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether the plurality of atomic database events include an executable SQL statement that exploits a buffer overflow vulnerability in the database {See SHOSTACK, Table 1, wherein this reads over "Check for known bugs in the servers . . that are vulnerable to buffer overflow attacks" and "X-windows. Check for open permissions that allow snooping of remote X session, unpatched libraries and executables vulnerable to buffer overflow attacks"};
>
> preventing the executable SQL statement from executing {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method of "processing the plurality of database events by detecting whether an executable SQL statement exploits a buffer overflow vulnerability in the database," SHOSTACK discloses a method of check for buffer overflow vulnerabilities. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

15. **Claim 100** is rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Reshef et al (U.S. Patent No. 6,321,337, hereinafter referred to as RESHEF), filed on 9 September 1998, and issued on 20 November 2001.

16. **As per dependent claim 100,** BAPAT, in combination with RESHEF, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing futher comprises the steps of:
>
> detecting whether an executable SQL statement includes an operating system call {See RESHEF, C10:L 21-35, wherein this reads over "[a]ny breach of the permitted flow sequences by disorderly operating system calls or looping will be trapped and logged"};
>
> preventing the executable SQL statement from making the operating system call {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method of "detecting an executable statement includes an operating system call," RESHEF discloses a method of checking for operating system calls which result in a breach of permitted flow sequences. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by RESHEF.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

17. **Claims 102-104** are rejected under 35 U.S.C. 103(a) as being unpatentable over BAPAT as applied to claims 89 and 90, and further in view of Rowland (U.S. Patent No. 6,405,318, hereinafter referred to as ROWLAND), filed on 12 March 1999, and issued on 11 June 2002.

18. **As per dependent claim 102,** BAPAT, in combination with ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether an executable SQL statement alters a set of auditing configurations existing on the database {See ROWLAND, C5:L61-67, wherein this reads over "name a local directory in an odd way to hide their work"};
>
> preventing the set of auditing configurations from being altered {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with auditing settings," ROWLAND discloses a method wherein suspicious directory activity is detected {See ROWLAND, C5:L61-67}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

19. **As per dependent claim 103,** BAPAT, in combination with ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises the steps of:
>
> determining whether an executable SQL statement includes a write operation to a set of audit records existing in a log file {See ROWLAND, C6:L4-11, wherein this reads over "[t]he system checks to determine if the system audit records have been altered or are missing"};
>
> preventing the audit records existing in the log file from being written to {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is interfering with audit records," ROWLAND discloses a method wherein "[t]he system checks to determined if the system audit records have been altered or are missing" {See ROWLAND, C6:L4-11}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

20. **As per dependent claim 104,** BAPAT, in combination with ROWLAND, discloses:

> The computer readable medium having code to perform the computer implemented method for protecting the database of Claim 98, wherein the step of analyzing further comprises:
>
> the steps of: determining whether an executable SQL statement includes an attempt by a user to obtain administrator access by changing a configuration file in the database {See ROWLAND, C5:L53-56, wherein this reads over "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred"};
>
> preventing the configuration file in the database from being changed {See BAPAT, C12:L19-26, wherein this reads over "[i]f a match is found, the request is denied, and a response is returned to the initiator if appropriate"}.

While BAPAT fails to expressly disclose a method "wherein said unauthorized activity is modifying security settings," ROWLAND discloses a method wherein "[t]he system examines the rhost file and other system authentication files to determine if dangerous security modifications to the host file have occurred" {See ROWLAND, C5:L53-56}. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by BAPAT by combining it with the invention disclosed by ROWLAND.

One of ordinary skill in the art would have been motivated to do this modification so that suspicious or malicious activity may be detected and prevented accordingly.

Response to Arguments

21. Applicant's arguments filed 23 January 2008 have been fully considered but they are not persuasive.

a. Claim Rejections under 35 U.S.C. 102(b)

Applicant asserts the argument that "Bapat does not anticipate the limitations concerning the listener agent and its relationship with the console." See Amendment, page 16. The Examiner respectfully disagrees. Applicant is directed to Figure 9 which discloses a set of filters 291, 294 in the log server 290 which determine which event notifications are stored. See Bapat, col. 16, line 62 – col. 17, line 1. Furthermore, it is noted that the log server is a software entity or process that runs on the same computer or computer node as the MIS. See Bapat, col. 16, line 64-66. Accordingly, it is noted that wherein the filter (i.e. the listener agent) is installed on the log server (i.e. the server hosting the database) and wherein the log server is a part of the MIS, the log server would inherently have established a secure connection between the MIS (i.e. the console) and the filter.

Secondly, Applicant asserts the argument that Bapat's disclosure of a filter passing "access grant" and "access denail" event notifications reads upon the claim limitations. See Amendment, page 16-17. The Examiner respectfully disagrees in that the Bapat would read upon the claims, as recited, in that Bapat discloses that the security alarm filter is used to identify a user that initiated each denied access request. Accordingly, one of ordinary skill in the art would have been able to correlate the cited prior art to read upon the limitation wherein the listener agent has a set of rules having a set of security attributes.

Thirdly, Applicant asserts the argument that Bapat's disclosure of collecting "access grant" and "access denial" event notifications reads upon the claimed method step of "installing a collector agent to be in communication with the listener agent for collecting a plurality of database events." See Amendment, page 17. The Examiner respectfully disagrees in that Bapat's disclosure of "a conventional database management system (DBMS) 280 for store event logs, 292, each of which stores even' notifications to which various users have requested directed SQL type access" would read upon said claimed method step.

Fourthly, Applicant asserts the argument that Bapat fails to disclose the limitation of "deconstructing the plurality of database events into a plurality of atomic messages." See Amendment page 17. The Examiner respectfully disagrees. Applicant is directed to Bapat's disclosure of "log server 290 whose primary function is to convert event notifications into SQL insert statements for storing event notifications in the event log." See Bapat, col. 16, lines 32-39. Accordingly, it would have been obvious to one of ordinary skill in the art that wherein the log server converts the event notifications into SQL insert statements, Bapat would indeed disclose a method wherein database events are deconstructed into atomic messages such as insert statements.

Fifthly, Applicant asserts the argument that the limitation of "executing compliant database events, depends on the term 'compliant' in the context of analysis of atomic messages." See Amendment, page 17. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "compliant" in the context of analysis of atomic messages) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Additionally, Applicant asserts the argument that Bapat fails to teach the method step of "sending a signal to a console operator when a database event is not compliant with the first set of rules." See Amendment, page 18. The Examiner respectfully disagrees. It is noted that Bapat discloses a method wherein "security alarms are generated and stored in the log only when there is a denial of object access." See Bapat, col. 17, line 15-21. Furthermore, it is noted that Bapat discloses that event notifications are forwarded to user and entities which have request a copy of said event notifications. Accordingly, it would have been obvious to one of ordinary skill in the art that the console operator would receive a notification (i.e. a signal) that a database event did not comply with a set of rules.

Additionally, Applicant asserts the argument that "[t]he general proposition that someone is authorized to modify the access control tree of Bapat is not the step of allowing a console operator to create exceptions." See Amendment, page 18. The Examiner respectfully disagrees. It is noted that wherein log server filters (i.e. a set of rules) are used by a user to filter database events, the modification by said user of the access control object tree which defines which events are to be stored in the event log would properly read upon the method step of creating exception to a set of rules. That is, the user may customize which event notifications are and are not to be transmitted or logged (i.e. creating exceptions).

Lastly, Applicant asserts the argument that "[t]he cited portion of Bapat does not disclose storing the signals received by the console operator, nor that the data file resides with the console." See Amendment, page 18. The Examiner respectfully disagrees. It is noted that wherein the MIS stores summary information about access request grants and denials, one of ordinary skill in the art would have readily been able to read said disclosure upon the recited claim limitation of storing signals received by the console operator.

For the aforementioned reasons above, the rejections under 35 U.S.C. 102 are maintained.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to PAUL KIM whose telephone number is (571)272-2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tony Mahmoudi can be reached on (571) 272-4078. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tony Mahmoudi/
Supervisory Patent Examiner, Art Unit 2169

Paul Kim
Examiner, Art Unit 2169
TECH Center 2100

/pk/